

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

25 January 1984
DCISEC-CSS-M160

1. The One Hundred and Sixtieth meeting of the Computer Security Subcommittee was held on 17 January 1984 at the [redacted] McLean, VA. The following persons attended:

STAT

STAT

STAT

STAT

STAT

[redacted] Executive Secretary

25X1

Mr. Dave Jones, DoE

Ms. Martha Tofferi, Air Force

Mr. Robert Graytock, Dept. of Justice

[redacted] NSA

25X1

Ms. Sue Berg, Navy

Mr. David Schencken, Secret Service

[redacted] SECOM Staff

25X1

[redacted] DCI (recently SECOM staff)

2. The minutes of the previous meeting were reviewed, and were accepted as written. It should be noted however, that the date for the minutes should be 1984.

3. The Subcommittee recognized Martha Tofferi as the new Air Force member. She replaces Mr. Lynn Culkowski, who has changed assignments within the Air Force.

4. Mr. Jones commented on the list of SOIC's that was attached to the minutes of the last meeting, pointing out that the SOIC for the Department of Energy may have changed. This led to a further discussion on the SOIC vs. the NFIB member. It was agreed that the Subcommittee would request the SECOM to provide a definition of SOIC, a complete list of SOIC's, identify those who have DCID authority, and identify the mechanism by which one determines which SOIC's have authority/responsibility for any given area (e.g., personnel security, physical security, computer security).

5. The Executive Secretary discussed the January SECOM meeting, which he attended in place of the CSS Chairman, who was not able to attend. He reported that [redacted] presented to the SECOM the same briefing which had been given to the Seniors on 28 November 1983. [redacted] who had also attended the SECOM meeting, provided some details of that briefing. He noted that [redacted] briefing states that the main focus of the technical effort is to provide fixes and short-term solutions, as opposed to addressing long-term, generic R&D. He also pointed out that the funds allocated by the project for fy 85 are not additional funds which have been added to the budget, but rather the intent is to indicate the level of effort required and to provide visibility for computer security related expenditures. Otherwise,

STAT

STAT

STAT

25X1

25X1

25X1

STAT the expenditures are expected to be absorbed by the individual agencies/departments. At the conclusion of the briefing [] 25X1
 was asked what impact she perceived her effort would have on the rewrite of DCID 1/16. Her response was that her policy-level recommendations will deal with issues such as bilateral agreements between Intelligence Community agencies. However, the Subcommittee noted the work of the Safeguards Group, who have defined a set of criteria for evaluating the "critical systems". Since these criteria have not yet been seen by the Subcommittee, then it was not yet clear whether or not they are relevant to the rewrite effort and, if so, exactly what impact they will have. It was agreed that the criteria needed to be reviewed, and [] 25X1
 agreed to make them available, to be distributed as an attachment to these minutes. It was also clear that the Policy Group established by the [] effort, under the chairmanship of [] 25X1
 [] should be consulted to determine the relevance and impact of their findings on the DCID 1/16 rewrite. 25X1

STAT 6. The majority of the meeting was spent on discussing the SECOM proposal for the rewrite of DCID 1/16 (which was attached to the minutes of the previous meeting, M159). With regard to the policy statement itself, the sense of the Subcommittee was that the only real difference was the inclusion of a set of specific mechanisms (in section 4), which were felt to be at too low a level to be included into a statement of high level policy. Thus, it was agreed to maintain the policy statement as originally proposed by the Subcommittee. However, it was recognized that the SECOM proposal for the policy statement incorporated some improved construction and terminology, and that these areas will be reviewed with a view to improving the wording. There was considerable discussion over the regulatory section. [] 25X1
 provided a detailed description of, and the motivation for, the drastically revised regulation. He stated that for the most part, the wording of the detailed requirements were taken directly from the Subcommittee's draft. There were numerous comments on the new regulation, which will not be reproduced here, but which led to the realization that the problems/issues that were being raised were caused precisely by lifting wording from the Subcommittee's draft and incorporating them into a new framework. That is, the Subcommittee's draft looks at the world from the perspective of user functionality and computer system environment (i.e., modes of operation), which also include hardware/software capability. The SECOM proposal however, approaches the problem from the perspective of a three dimensional matrix whose axes are user clearance, data classification, and handling restrictions (including caveats, "bigot lists", and compartments). Thus, since the two approaches are fundamentally different, one would expect the specific wording of requirements to be different. Clearly then, trying to use the requirements statements from the one framework in a different structure was going to cause things to appear out of their intended (and proper) context. It was agreed that there was no basic disagreement with the intended approach (i.e., the matrix) being proposed, but that a radically new structure was going to require a complete rewrite of the content in order to clearly and adequately specify the level of security

intended. The discussion concluded with the resolution that the Executive Secretary would provide the Chairman with the results of these discussions so that he can, in turn, report the Subcommittee's position on the rewrite issue at the next meeting of the SECOM.

STAT

7. [] provided some clarification on the issue of the classification of the DCID's. He stated that the original decision was that all DCID's will be classified by default, but that a specific DCID could be classified lower, or even be published as unclassified, as the circumstances dictated. He stated that if the Subcommittee felt that the classification of the DCID was inappropriate, all that was necessary was for the Subcommittee to present its case formally. 25X1

STAT
STAT

8. The next meeting of the Computer Security Subcommittee will be held on Tuesday, 21 February at 0930 at [] McLean VA. The members should be prepared to discuss the DCID rewrite in further detail, specifically: 25X1

(a) final decision on which version of the policy paper will be adopted, as well as the detailed comments on the content.

(b) final decision on which approach is to be adopted for the regulation, also to include detailed comments on content.

STAT

[] 25X1

~~CONFIDENTIAL~~

30 JAN 1984 17

THE WHITE HOUSE
WASHINGTON

~~CONFIDENTIAL~~

January 30, 1984

MEMORANDUM FOR THE SECRETARY OF STATE
 THE SECRETARY OF THE TREASURY
 ✓ THE SECRETARY OF DEFENSE
 THE ATTORNEY GENERAL
 THE SECRETARY OF COMMERCE
 THE SECRETARY OF TRANSPORTATION
 THE SECRETARY OF ENERGY
 THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
 THE DIRECTOR OF CENTRAL INTELLIGENCE
 CHAIRMAN, JOINT CHIEFS OF STAFF
 ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION
 DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
 DIRECTOR, NATIONAL SECURITY AGENCY
 MANAGER, NATIONAL COMMUNICATIONS SYSTEM

SUBJECT: National Policy on Telecommunications and
 Automated Information Systems Security (U)

Enclosed for your review is a proposed draft NSDD to replace the current PD/NSC-24, Telecommunications Protection Policy, November 16, 1977. (C)

The proposed NSDD accommodates a number of important goals:

- It continues efforts and programs begun under PD-24, including PD-24's focus on protection of systems handling both classified and other sensitive information and sensitive non-government information. (C)
- It provides a broad-based organizational framework for developing and overseeing national policy in this area on behalf of the National Security Council and the President. (U)
- The structure proposed in this draft seeks to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat, and to foster an appropriate partnership between government and the private sector in attaining these goals. It specifically recognizes the special requirement for protection of intelligence sources and methods. (C)

I-06986/84
 X29128

SEC DEF CONTR No.

~~CONFIDENTIAL~~

4 15
 1000

- The new structure is intended to replace both the PD-24 Interagency Group for Telecommunications Protection (IG/TP) and the National COMSEC Committee (NCSC). (C)

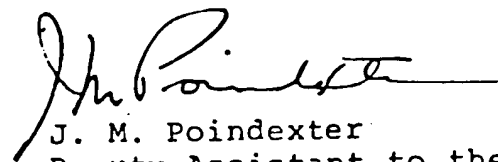
- It establishes a mechanism for evaluating the overall effectiveness of programs and resources and for establishing national priorities and effective levels of investment. (C)

- It consolidates executive agent responsibilities and assigns specific implementation authorities so as to assure effective and efficient administration of policy. (U)

- It explicitly combines telecommunications security and automated information systems security under a single national policy umbrella. This combination represents a significant enhancement of the PD-24 policy structure and is predicated on the Nation's need to assure equivalent and compatible security policies, standards, and postures in the two areas as their underlying technologies converge. (C)

The draft NSDD recognizes that while we have considerable experience in telecommunications security, we are only beginning to understand all aspects of automated information systems security. Also, there are substantial differences in the level of maturity of the various security technologies. Since continuing advances in technology can be expected to influence the implementation and future direction of policy in this critical area, the NSDD is framed to accommodate the possibility of changes, in either focus or structure, as needs dictate. Therefore, the NSDD establishes a forward-looking policy development and implementation structure which is sufficiently broad to adapt to future developments in automated information systems security. For example, it is expected that policy in this area will be strongly guided by studies currently underway, such as the intelligence community's review of computer security being conducted by the Davis panel. It is intended that the machinery established by this NSDD would initially focus on those automated systems which are connected to telecommunications transmission systems. (C)

A working group meeting to discuss the enclosed draft is scheduled for Friday, February 17, 1984, at 1400. Please designate a representative to attend this session and act as your point of contact for ensuing coordination actions. The names of working group representatives should be provided to Mr. Kenneth E. deGraffenreid (395-3334) of the NSC Staff. (U)



J. M. Poindexter
Deputy Assistant to the President
for National Security Affairs

Attachment
Draft National Security Decision Directive

CONFIDENTIAL

4 15 1000

CONFIDENTIAL

THE WHITE HOUSE

WASHINGTON

DRAFTCONFIDENTIAL*National Security Decision
Directive Number*NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the demand for telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, electronic penetration, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. (C)

These systems process and communicate classified national security information, other sensitive information concerning vital interests of the United States, and the private information of US persons and businesses. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its interests. A comprehensive and coordinated approach must be taken to protect the Nation's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. (C)

This Directive provides initial objectives and policies to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information, establishes a mechanism for policy development and assigns responsibilities for implementation. (U)

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities

CONFIDENTIAL

Declassify on: OADR

CONFIDENTIAL

CONFIDENTIAL

2

of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, other sensitive government information, and certain private information of US persons is a key national responsibility. I, therefore, direct that the Nation's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained and improved as necessary to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government and private resources.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems. (U)

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secure or protected by such means as are necessary to prevent compromise and exploitation.

b. Systems handling other government-derived information, the loss of which could adversely affect the national interest or the rights of US persons, shall be protected in proportion to the threat of exploitation and the associated potential damage.

c. The government shall take necessary steps to identify systems which handle non-government information, the loss of which could adversely affect the national interest or the rights of US persons and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national interest, the private sector shall be encouraged and assisted in undertaking the application of such measures. (U)

CONFIDENTIAL

CONFIDENTIAL

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies. (U)

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of Defense, the Secretary of the Treasury, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the National Manager with respect to the activities undertaken by him in implementing this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of national telecommunications and automated information systems with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review and approve consolidated resources program and budget proposals, and other matters referred to it by the Executive Agent in fulfilling his responsibilities outlined in paragraph 6. below.

(5) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(6) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(7) Recommend for Presidential approval additions or revisions to this Directive as national interests may require. (U)

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group. (U)

CONFIDENTIAL

CONFIDENTIAL

4-15
7000

~~CONFIDENTIAL~~
CONFIDENTIALCONFIDENTIAL

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by a representative of the Secretary of Defense and shall be composed of a non-voting representative of each member of the Steering Group and a voting representative of each of the following:

The Secretary of State
The Secretary of the Treasury
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
The Director of Central Intelligence
Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Director, National Security Agency
Manager, National Communications System (U)

b. The Committee shall:

- (1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.
- (2) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.
- (3) Approve the release of sensitive systems security information, techniques and materials to foreign governments or international organizations (except in intelligence activities managed by the Director of Central Intelligence).
- (4) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.
- (5) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.
- (6) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures

CONFIDENTIAL

4 15 1060

~~CONFIDENTIAL~~
CONFIDENTIAL

for permanent observers, from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman. (U)

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on information processing security. Recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate and shall consider any differences in the level of maturity of the technologies to support such implementations. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important. (U)

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency. The secretariat may be augmented as necessary by personnel provided by the departments and agencies represented on the Committee in response to the Chairman's request. The National Security Agency shall provide facilities and support as required. (U)

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with the National Manager and with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the formulation of necessary security architectures.

b. Fulfill requirements of the government for technical security material and related services.

c. Approve and provide minimum security standards and doctrine.

d. Conduct or approve research and development of security techniques and equipment.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Procure for and provide to government agencies, and, where appropriate, to private institutions (including

CONFIDENTIAL

government contractors) and foreign governments, equipment and other materials as required to accomplish the objectives of this Directive.

g. Develop and submit to the Steering Group a proposed National Telecommunications and Information Systems Security Program budget for each fiscal year, including funds for the procurement and provision of equipment and materials.
(U)

7. The National Manager for Telecommunications and Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Information Systems Security and is responsible for carrying out the foregoing responsibilities of the Secretary of Defense as Executive Agent. In fulfilling these responsibilities the Director, National Security Agency shall have authority to:

a. Examine government telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with the law and other applicable directives.

b. Act as the government focal point for all matters related to cryptography, communications security, and the security of automated information systems. Responsibilities shall include conducting or approving all research and development; reviewing and approving all standards, techniques, systems and equipments; and conducting liaison, including agreements, with foreign governments, international and private organizations.

c. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other sensitive technical security materials or services.

d. Operate a central technical center to assess and disseminate information on hostile threats to national telecommunications and information systems security and to assess the overall security posture.

e. Operate a central technical center to evaluate and certify the security of telecommunications systems, and automated information systems, and to conduct or sponsor research and development of security techniques.

f. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

CONFIDENTIAL

CONFIDENTIAL

7

CONFIDENTIAL

g. Review annually the systems security program and resources requirements of the departments and agencies of the government, and prepare consolidated National Telecommunications and Information Systems Security Program budget recommendations.

h. Request from the heads of departments and agencies such information and technical support as he may need to discharge the responsibilities assigned herein.

i. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations (including government contractors) and foreign governments. (U)

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining an acceptable security posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, the Secretary of Defense as Executive Agent, and the Director, National Security Agency as National Manager, as appropriate, such information as they may require to discharge responsibilities assigned herein. (U)

9. Additional Responsibilities.

a. The Director of Central Intelligence shall coordinate with the Steering Group, NTISSC, and the Director, NSA, as appropriate, concerning unique requirements pertaining to the protection of intelligence sources and methods.

b. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use standards for the security of telecommunications and other automated information systems as the Director, NSA may approve.

c. The Director, Office of Management and Budget shall review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.
(U)

10. Nothing in this Directive:

CONFIDENTIAL

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel or facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for purposes not provided for herein.

c. Amends or contravenes the provisions of existing directives which may pertain to the financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems. (U)

11. For the purposes of this Directive, the following terms shall have the meanings indicated.

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and the protection of sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of

CONFIDENTIAL

telecommunications and automated information processing systems. (U)

12. The Interagency Committee on Foreign Real Estate Acquisitions in the United States established under Presidential Directive 24 shall be reconstituted to serve as an interagency policy coordination committee under the chairmanship of the Department of State, with representation from the Department of Defense, the Department of Justice/Federal Bureau of Investigation, the Director of Central Intelligence, the National Security Agency, and the Assistant to the President for National Security Affairs. It shall provide policy guidance for implementation by the Office of Foreign Missions of the Department of State or other appropriate organizations on proposals for foreign real estate acquisitions, by lease or purchase, that present a security threat to US telecommunications and automated information systems or are of counterintelligence interest. (U)

13. The functions of the National Communications Security Committee (NCSC) are subsumed by the NTISSC. The policies established under the authority of the NCSC shall remain in effect until rescinded or modified by the NTISSC. (U)

14. Except for ongoing telecommunications protection activities mandated by and begun under PD/NSC-24, that Directive is hereby superseded and cancelled. (U)

CONFIDENTIAL

CONFIDENTIAL

4 15
(1000)